LA-UR-03-2381

*Approved for public release;
distribution is unlimited.*

Title:

Using Safety Tools to Improve Security

Author(s):

Daniel J. Pond

Submitted to:

International System Safety Conference
August 4-8, 2003
Ottowa, Canada

Using Safety Tools to Improve Security

Daniel J. Pond , Ph.D.; Los Alamos National Laboratory; Los Alamos, NM

Keywords: human error, security

Abstract

Human error assessment and other safety analysis tools reveal that worker errors contributing to or resulting in accidents are often the consequence of ineffective system conditions, process features, or individual employee characteristics. At Los Alamos National Laboratory (LANL), a team of security, safety, human error, and organizational experts considered whether the *system-induced human errors* that make accidents more likely could also be contributing factors to security incidents. Because our review of more than 100 such incidents suggests they can and do, LANL has adapted error assessment tools and reduction techniques for application to security tasks and operations. Safety professionals--especially those with human error assessment and mitigation expertise--have the knowledge and skills needed to apply these tools in enhancing security in their own organizations.

Introduction

Elimination of all security incidents has not proven possible by a "gates, guards, and guns" approach in tandem with such traditional interventions as general security training or progressively harsher exemplar disciplinary actions. To address this situation, LANL has adapted safety-based assessment tools and techniques for application to tasks in which improper or ineffective performance has security implications. Specifically, by identifying the factors that make errors and the resulting security incidents more likely, mitigation strategies that effectively target these contributors can be developed. Overall security is enhanced not only by, for example, minimizing the inadvertent release of classified information through errors, but also by reducing the security resources devoted to these activities, thereby permitting limited resources to be directed toward prevention of- and response to- other security threats.

Human Errors in Safety and Security Applications

Safety and Human Error: In 1999, the Institute of Medicine reported that as many as 98,000 hospitalized Americans die and another 1 million are injured each year as a result of preventable errors (ref. 1). As many as 70% of electronic equipment failures and 90% of air traffic control errors have been found to have human origins, and error rates for something as simple as reading instructions have been found to be as high as 6.5% (ref. 2). While Hollnagle (ref. 3) reported that the contribution of human error to accidents in applications ranging from air transport operations to nuclear power plants was about 80% in 1990, he notes that the trend has been steadily increasing since the 1960s owing to greater system complexity (resulting in more errors), improved error analysis methods (improving our error detection capability), and other factors, many of which are likely to apply to security operations as well.

A sizable number of tools to assess error probabilities have been developed, dating back at least 40 years. Among the most well known of these are the Technique for Human Error Rate Prediction (THERP), its streamlined descendant, the Accident Sequence Evaluation Program (ASEP), the Human Error Assessment and Reduction Technique (HEART), and the Generic Error Modeling System (GEMS) (see ref. 4 for a comparative discussion). Some of these assessment techniques focus on errors in specific domains such as nuclear power plant operations or aircraft maintenance, while others were developed or subsequently modified to be more broadly applicable.

While it's undoubtedly true that human errors can never be completely eliminated, the good news is that those "induced" by various system characteristics--including the human as a system component--can be reduced through traditional systems analysis, hazard assessment, and human error mitigation techniques. But to do so we must first discover and recognize the potential influence of these *system* factors on worker performance. Indeed, Dekker (ref. 5) asserts that the new view of human error is that it is not a cause of system failure but, rather, a "symptom of trouble deeper inside the system." As case in point, a newspaper reported the crash of a US Army helicopter during training maneuvers. While the article notes problems associated with exterior and interior design features, lack of lighting, and limited pilot training, the headline read "Pilot Error Blamed for Helicopter Crash" (ref. 6). If this headline reflects the conclusion of the accident review team, the stage may have been set not only for unjust disciplinary action but also, by discounting the importance of relevant contributing factors, for ineffective remediation and prevention of future occurrences.

Most assessment techniques attempt to account for variables or conditions that influence the likelihood of errors occurring; these have been referred to as Performance Shaping Factors (PSFs), Error Producing Conditions (EPCs), and Error Shaping Factors (ESFs), among other terms. Such conditions can lead directly and immediately to operator errors, or can be "latent" conditions that are benign for long periods before combining with other conditions or events to induce errors (ref. 7). Although pilot- and operator-errors certainly do occur, many so-called human errors that result in undesirable actions are instead near-inevitable consequences of ineffective system conditions, process features, or individual employee characteristics; the proverbial "accident waiting to happen." For present purposes the question is, if certain EPCs make an accident more likely in one circumstance (for example, while operating a forklift), could they make a security incident more likely in other contexts (for example, while handling classified material)? In other words, can the factors known to contribute to unsafe acts also contribute to acts that threaten the security of an organization or a nation? After reviewing more than 100 past security incidents, LANL's team of security, safety, human error, and organizational experts concluded they can and do.

Safety versus Security Applications:
The contribution of errors to both accidents and security incidents, the apparent commonality of contributors to these errors, and the fact that relatively few accidents and incidents result from workers' intentions to harm themselves, cause damage, or undermine national security, makes possible an "adapted safety practice" approach to reducing security incidents. There are, however, some important differences between these two areas of application. For example, accident consequences tend to be more immediately evident than those associated with security incidents, and accident impacts are more often more localized and repairable/recoverable than are security incident outcomes.

Further, diagnostic input from workers involved in accidents and near accidents is increasingly recognized as invaluable in eliminating the precursor conditions that contributed to the (near) event. As a result, many organizations have established no consequence policies for those who self-report, especially for first time offenders. On the other hand, actions contrary to security requirements are rarely met with forgiveness because such actions are often violations of law. This, of course, shifts the focus of post-event inquiries from *causes* to *culprits* which, in turn, can dramatically alter the nature of the discourse between investigators and involved individuals.

Security and Human Error: If we conservatively estimate that human error involvement in security operations is only two-thirds of that reported for accidents--as detailed, perhaps 80%--we're still left with human errors contributing to the majority of security incidents. With the increase in security focus, requirements, and consequences presented by today's world, it is essential that errors and their contributors be brought to the lowest levels possible.

"Failure to obtain a review" of documents, view graphs, or other media to ascertain the classification of the contents--for example, Unclassified, Confidential, Secret--and to thereby define the proper handling requirements, is among the most common (albeit still infrequent) event resulting in a security incident at LANL. Such a characterization is undoubtedly an accurate indication of what constituted this incident, and it may also provide sufficient basis for recommending disciplinary actions that may result. Additionally, the corrective actions plan may assert that "employees must remember to obtain required reviews" and "supervisors should remind employees to obtain reviews." A typical remediation action might be to "assure that Annual Security Refresher Training emphasizes the requirement to obtain reviews" and the employee might be disciplined by having the event become a part of his/her personnel record.

So, with this array of remediation responses in place, the issue is controlled, right? Perhaps. These steps might be successful if the source of the problem was that the employee never knew that reviews are required of all materials prior to transmission in any form either within or outside the organization (unlikely), or didn't remember this requirement (possibly). But what if the failure to obtain a review was influenced by the unavailability of a qualified reviewer within the required timeframe? Or what if pressure to meet a project deadline was exerted by a supervisor? Or suppose it was known that a nearly identical previous version of the document had been reviewed a few days earlier and judged to be Unclassified? Clearly, if we're going to be able to fix a problem, we've got to understand what the problem really is, and we've got to have tools suitable to the task.

ESTHER

LANL's team of security, safety, human error, and organizational experts focused on actions comprising and circumstances surrounding each of 100+ incidents which took place during the period FY 1999 through FY 2001. Not surprisingly, although the inquiry reports were typically comprehensive in addressing what happened, discussions of why it may have happened were generally less extensive, and indications of factors that contributed to the event were included even less frequently. As a result--based only on the information in the inquiry reports and using accident contributor factor lists to stimulate thought and discussion--the team developed expert judgment assessments of *plausible* contributors to the actions which led to or constituted each security incident. Table 1 details the 15 situational- and 12 personal- error contributing factors defined, with a security-relevant example of each provided (additional examples can be found in ref. 8). These factors comprise the central component of ESTHER--Enhanced Security Through Human Error Reduction--and LANL's efforts to reduce the number and, especially, recurrence of security incidents.

By comparison, note that some safety-focused error *causal factor* taxonomies are highly detailed. For example, Maurino, Reason, Johnston, & Lee (ref. 9) define 26 situational- and 30 personal- factors that underlie human error and "contribute to unsafe acts." On the other hand, the US DOE Incident Tracking & Analysis Center (http://www.pnl.gov/isrc/itac.stm), which was established to coordinate, analyze, and archive security incident data, has developed an Incident/Inquiry Report to assist in obtaining accurate and thorough information regarding an incident of security concern. While this form provides 55 categories of potential incident consequences, it considers only 9 types of "fundamental (root) causes(s)," one of which is Personnel Error. ESTHER seeks to enable the broadest coverage of factors potentially contributing to security incidents with the fewest number of clearly differentiated contributors. It is expected that the current list of 27 factors may change over time, and it's intended that quantitative and qualitative adaptations will made to suit each implementation.

Table 1 - Error-Contributing Factors to Security Incidents

Situational	
Distractions	Question from colleague
Job Pressure	Competing demands (e.g., security compliance vs. deliverable timeliness)
Time Factors	Day before or after weekend, vacation, holiday
Task Complexity	Detection of unspecified contraband using x-ray equipment
Task Aversive-ness	Repetitive tasks, such as signing off after each safe opening and closing
Routines Changed	Transfer to an organization with different practices
Inadequate Information	Accumulation of unclassified information yields a classified product
Procedures/Directions	Nonexistent, unavailable, inaccurate, or ambiguous guidance
Communications	No mutual understanding about day's end responsibility for classified materials
System Status/Feedback	Not readily apparent if media is in computer or storage container
Material/Resources	No provision for indication of safe closure status
Work Planning	Failure to plan for adequate Classification review periods
Environment	Classified computer screen visible to staff who do not have "need to know"
Management / Systems	Staffing mix inappropriate for task ; training course deficiency
Culture/Local Practices	Pattern of unconcern about security and safeguard requirements
Personal	
Preoccupation/Inattention	Focus on other project/technical work
Stress/Anxiety	Personal problems (e.g., financial concerns, domestic strife, sick child)
Fatigue/Sleeplessness/Boredom	Jet lag
Illness/Injury	Headache
Drug Side Effects	Drowsiness
Ability	Short employee unable to accurately determine if top safe drawer is locked
Experience/Skills	Novice unfamiliar with procedures/practices
Knowledge	Absent, incomplete, or incorrect understanding about laptop microphone
Misperception	Mis-heard agreement about transfer of safe closing responsibility
Memory Failure	Cell phone inadvertently brought into a secure area
Reasoning/Judgment	Document assumed to be unclassified because it was formerly unclassified
Values, Beliefs, Attitudes	Supervisor's cavalier approach leads to a poor security culture among staff

Every effort was made to include terms based on their most common usage. However, in a few instances it was necessary to instead use narrower or specialized definitions used in human error and other behavioral assessments (see Glossary). For example, effective ESTHER implementation will require an understanding of the way *(mis)perception* is used here, as well as the distinction between *ability* and *skill*.

<u>Errors and Breaches</u>: At the simplest level, error classification schemes distinguish between actions performed properly, something done incorrectly (errors of commission) and something not done (errors of omission). Expansions of these categories enable consideration of something done correctly but at the wrong time, and failure to perform one step of an operation, among other error types. An alternative approach parses errors according to whether the tasks can be accomplished without conscious control (skill-based), rely upon mentally-stored rules or procedures (rule-based), or require application of thought, planning, or reasoning (knowledge-based). None of these taxonomic approaches is inherently correct or incorrect, nor universally better or worse. To be most useful, these and other assessment tools must be tailored to specific applications. Based on the kinds of incidents identified by LANL's team, the ESTHER program focuses on four kinds of errors:

- unintentional acts ("I didn't mean to do that")
- unintentional failures to act ("I forgot to do that")
- intentional but incorrect acts ("I thought that's what I was supposed to do")
- intentional but incorrect failures to act ("I didn't think I was supposed to do that").

In addition, it is recognized that some proportion of security incidents is the result of deliberate deviations from required policies and practices; these are termed *breaches* here. It is important to note that this category includes only deliberate *non-malevolent* deviations. Espionage and other actions taken to undermine national security are beyond the scope of ESTHER; other programs must be in place to address such problems. Table 2 provides an example of a breach for each of the relevant situational and

Table 2 - Breach-Contributing Factors to Security Incidents	
Situational	
Distractions	N/A
Job Pressure	Shortcut taking or other deviations from required procedures prompted by competing demands (e.g., security compliance vs deliverable timeliness)
Time Factors	Shortcut taking or other deviations from required procedures prompted by, for example, end of shift, classified material courier waiting
Task Complexity	Shortcut taking or other deviations from required procedures to simplify task or streamline procedures perceived as extraneous to task
Task Aversive-ness	Shortcut taking or other deviations from required procedures to avoid perceived “no value added” task
Routines Changed	Failure to follow new procedures, choosing instead—e.g., for convenience—to use those as implemented in previously-assigned organization
Inadequate Information	N/A
Procedures/Directions	Shortcut taking or other deviations from required procedures prompted by procedures believed to be incorrect
Communications	N/A
System Status/Feedback	N/A
Material/Resources	Shortcut taking or other deviations from required procedures prompted by unavailability of proper classified material marking/packing supplies
Work Planning	Failure to adequately perform *required* planning operations in order to save time or effort
Environment	Shortcut taking or other deviations from required procedures prompted by adverse weather
Management / Systems	Shortcut taking or other deviations from required procedures prompted by inequitable disciplinary actions for security infractions
Culture/Local Practices	Shortcut taking or other deviations from required procedures prompted by a pattern of inconsistent enforcement of security requirement in the organization
Personal	
Preoccupation/Inattention	N/A
Stress/Anxiety	Cover up of an error-based security incident because of fear of consequences
Fatigue/Sleeplessness/Boredom	N/A
Illness/Injury	Failure to check bottom drawer of safe because of difficulty in bending associated with arthritis
Drug Side Effects	Impairment of reasoning or judgment
Ability	Inadequacy in a particular area leads an individual to compensate by deviating from a procedure. For example, an employee with weak language or reading skills resorts to memorization *instead of following written procedures as required*
Experience/Skills	Lack of proficiency with computer system leads one to leave hard drive in computer overnight
Knowledge	N/A
Misperception	N/A
Memory Failure	N/A
Reasoning/Judgment	Transmit document without classification review because contents are thought to be unclassified
Values, Beliefs, Attitudes	Cover up or fail to report possible security incidents because, for example, of friendship with or loyalty to the individual(s) involved

personal contributing factors.

Those familiar with human error analyses will note that we are using the term *breaches* in a manner similar (although not identical) to the way *violations* has been employed in safety applications. This change was necessary because in safety practice "...violations can be defined as deliberate—but not necessarily reprehensible [emphasis added]—deviations from those practices deemed necessary (by designers, managers, and regulatory agencies) to ensure the safe operation of a potentially hazardous system" (ref. 10). In predominantly law-based security operations, however, deliberate deviations are almost never appropriate or tolerated, no matter how well-intentioned.

On the other hand, violations and breaches are similar in a number of significant respects. For example, violations are known to increase the inevitability or severity of accidents by expending the "margin of error" designed into the system or by negating the recoverability of erroneous actions that may follow. Consequently, failing to use a safety harness when working on an elevated platform (violation of a safety rule) can mean that a simple slip (error) results in death rather than a sprain or a few bruises. Similarly, preparing a classified document on an unclassified computer (breach of a security requirement) can have dire national security consequences if this document is then mistakenly attached to an email message (error) and transmitted. In the absence of this breach, the error would not have occurred and no release of classified information taken place because protections against such inadvertent transmittals are built into LANL's classified computing network. Additionally, Maurino, et al. (ref. 9), with reference to safety applications) report

> *[w]hereas errors arise primarily from informational problems (i.e. forgetting, inattention, incomplete knowledge, etc.), violations are more generally associated with motivational problems (i.e. low morale, poor supervisory example perceived lack of concern, the failure to reward compliance and sanction non-compliance, etc.)...Errors can be reduced by improving the quality and the delivery of necessary information within the workplace. Violations require motivational and organization remedies.*

ESTHER presumes the contributors to breaches and the means with which to mitigate them are similar to those found for violations, and it provides the assessment capabilities to support such efforts.

ESTHER Implementation: ESTHER was designed to be used retrospectively as a tool to support and guide inquiries into security incidents that have taken place, and prospectively as a tool to support and guide efforts to reduce the likelihood of a security incident occurring. Such uses are, of course, direct corollaries to safety accident investigations and hazard assessments, respectively, with the information in Table 1 and Table 2 relevant whether one is "pulling the thread" as part of an inquiry into a specific event or analyzing the incident potential of a situation in which classified work will be performed.

In either application, a finding of multiple contributors is likely, but perhaps especially so for prospective applications in which potentially-numerous eventualities must be considered. Using the list of contributors as prompts to stimulate or direct the thoughts of individuals participating in incident potential assessments is strongly encouraged. On the other hand, such use with subjects of incident inquiries generally should be avoided or included only with careful planning and due caution to avoid "contaminating" the individuals' responses (that is, "leading the witness").

The information in Table 1 and Table 2 has been adapted into jobs aids, with retrospective/investigation functions supported by a *Field Guide* (ref. 11) and prospective/assessment use guided by a (currently draft) *Management Walk-Around Guidance Card* (see Figure 1). It is intended that these job aids be tailored to best accomplish the objectives and meet the needs of each organization by, for example, amending the examples and combining or expanding the list of factors.

Figure 1 - (Draft) Management Walk-Around Guidance Card

Number:	Functional Area:
Rev:	Topic: Employee Errors and Security Incidents

References: LA-UR-02-815 Rev., Enhanced Security Through Human Error Reduction

Performance Expectations

1. Staff are provided a workplace in which security issues are given suitable emphasis at all times; materials, equipment and other needed resources are readily available; environmental conditions are controlled to appropriate levels; and distractions from classified work are minimized.

2. Classified work is based on appropriate planning and performed without imposition of undue time constraints and programmatic or organizational pressures. Job assignments reflect consideration of staff knowledge, skills, and abilities relative to the difficulty of the task and worker familiarity with it. Less-favored task assignments are made equitably and managed effectively.

3. Staff are provided timely, accurate, and understandable guidance and status information--verbal, visual, numerical, textual--required to perform classified work.

4. Staff maintain self-awareness of personal circumstances which could impair their performance on classified work, and managers are alert to conditions or actions by staff which could indicate the potential of such impairment.

Procedure

- Review guidance card
- Observe classified work areas for conditions which could increase the likelihood of employee error
- Confirm currency of staff training and adequacy of capabilities to perform assigned classified work
- Interview staff regarding suitability of work environment, project demands, provided resources
- Observe staff for indications of conditions or actions which could be precursors of impaired performance
- Review classified information/material procedures for currency, clarity, and relevancy to staff activities
- Record observations and interview results
- Document results, including actions taken or planned

Questions

For Managers / Team Leaders

1. Are all workplace conditions conducive to error-free classified work?
2. Are all staff trained and otherwise capable of performing their assigned classified work?
3. Are all job conditions--e.g., project schedules and planning, clarity of assignments, adequacy of procedures, task difficulty, materials/equipment--effectively controlled?
4. What have you done most recently to convey the importance of security in your staff's classified work?

For Staff

1. What planning was done for the classified work you're now doing? Did your team leader or manager review this plan before you began work?
2. What are the applicable procedures, guidelines, or other requirements for the classified work you're now doing? Did you review this information before beginning work? Is this information clear, current, and readily accessible?
3. Do you have all the resources--e.g., time, materials, equipment, information--you need to perform this work effectively?
4. Is there anything, either on the job or off, that might keep you from performing this work with complete effectiveness today?
5. Does everyone involved with this task/project/group place adequate emphasis on security at all times?

It is essential that incident types are defined to effectively distinguish among different of actions that constituted or led to an incident. "Improper transmittal of classified information" is the incident category LANL used to describe such events as mailing classified material that has been improperly sealed as well as those in which an email with a classified document attachment is sent over a non-secure server. However, since the conditions, specific actions, and applicable requirements may be substantially different between these two, use of a common descriptor inhibits efficiently "pulling the thread" to discover the factors which contributed to the occurrence of either event. In turn, without discovery of such contributors our ability to effectively target needed solutions is undermined. That is, our response to ten "improper transmittal" incidents is likely to--indeed, must--differ if there are actually nine package sealing events and one email incident versus one of the former and nine of the latter. One might, therefore, consider establishing such categories as "Improper Packaging: Classified Documents" and "Improper Transmittal: Email" through which to address these incidents.

As behaviorally-relevant--as opposed to consequence-relevant--contributor/error/incident data come available, *risk categories* can be defined as is routinely done in safety applications--that is, the likelihood of occurrence multiplied by the severity of outcome. The contributors to high-likelihood incidents that have a high probability of resulting in compromised classified information or protected material are, of course, addressed first, with attention given last to low frequency-low consequence incidents. For most applications, the list of relevant contributors is likely to be very similar and, with appropriate tailoring of the associated examples, LANL's list should prove adequate for most initial implementations. Further, experience shows that once the list is made available many employees will view the error-inducing effects of the factors as common sense information and be comfortable from the outset with address these issues.

The organization's primary tasks are to provide the necessary clarification (most important, we've found, being the distinctions between errors and breaches), maintain staff awareness of these issues and, then, assure they have the resources with which to address them. Adding brief human error/breach modules to new hire orientation and periodic security refresher training courses are easy and effective ways to both educate and increase awareness. "Did you know...?" or "What's wrong with this picture?" photos or cartoons in company newsletters, security posters, or as computer start-up windows or screen savers can be light-hearted but nonetheless effective ways to keep employees vigilant.

Contributions of System Safety/Human Error Experts

Ways to minimize the influence of discovered contributing factors will in some cases be obvious and within the employees' control. These include such things as reducing clutter, improving work planning, assuring required materials are available before starting the task, and working in areas less likely to present distractions. On the other hand, control of such identified factors as improving procedures believed to be deficient, determining fitness to perform when taking certain prescription medications, or deciding if skill refresher training is needed, are likely to require involvement of line management. Interventions involving, for example, job re-design to eliminate overly-complex tasks, improving inappropriate local security cultures and practices, and dealing with management systems deficiencies, will probably require support of error assessment and mitigation experts, especially in the early stages of the error reduction program.

Conclusions

Employees can be enlisted into the security program in ways other than just as targets of myriad regulations and subjects of incident inquiries. By educating staff about the factors contributing to the errors and breaches that result in security incidents, then empowering them to "find 'em and fix 'em," the phrase "security is everyone's job" becomes more than just a slogan or words on a poster; employees are not only assigned responsibility for security, but also given the tools required to do the job. Many members of the System Safety Society are qualified to lead development of such programs, tailor the tools to each application, and provide technical leadership or support to the error analytic and correction efforts, thereby enhancing the safety professionals' organizational influence, impact and value.

ESTHER Glossary

Ability: Relatively enduring attributes of an individual, having both genetic and, usually to a lesser degree, learned components. Examples include depth perception, manual dexterity, and originality.

Breach: Deliberate deviation from policies, procedures, rules, directions, etc., with no intention to bring about any adverse consequence.

Contributors: Factors that can affect the likelihood of an error or a breach occurring in performance of security-related tasks.

Error: Unintentional failure of actions to be in accordance with required procedures or to achieve the desired consequences. These include failures to properly develop or execute a plan.

Misperception (perception): Incorrect (correct) detection, identification, and/or recognition of sensory (e.g., visual, auditory, tactile) information.

Personal: Individual employee traits (long-term characteristics or conditions) or states (transient characteristics or conditions).

Situational: Workplace or task conditions, circumstances, and/or features.

Skill: Level of proficiency on a task. Although largely a learned or acquired characteristic, it is often predicated in part on possession of relevant abilities. Examples include sealing a classified document mailing envelope (perceptual-motor skill) and understanding written security procedures (language skill).

References

1. Boodman, S.G. *No End to Errors*. Washington DC: Washington Post, December 3, 2002.

2. Dhillon, B.S. *Human Reliability with Human Factors*. Elmsford, NY: Pergamon, 1986.

3. Hollnagel, E. *Human Reliability Analysis: Context and Control.* London: Academic Press, 1993.

4. Kirwan, B. *A Guide to Practical Human Reliability Assessment*. Bristol, PA: Taylor & Francis, 1994.

5. Dekker, S. *The Field Guide to Human Error Investigations*. Burlington, VT: Ashgate, 2002.

6. Baltimore Sun. *Pilot Error Blamed for Helicopter Crash*. Baltimore, MD: Baltimore Sun, 7/2/88.

7. Reason, J. *Managing the Risks of Organizational Accidents*. Burlington, Vermont, Ashgate, 1995.

8. Pond, D. *Enhanced Security Through Human Error Reduction (ESTHER),* LA-UR-02-815. Los Alamos, NM: Los Alamos National Laboratory, 2002.

9. Maurino, D. E., Reason, J., Johnston, N., and Lee, R. B. *Beyond Aviation Human Factors*. Burlington, Vermont, Ashgate, 1995.

10. Reason, J. (1990). *Human Error*. Cambridge England, Cambridge University Press, 1990.

11. *ESTHER: A Field Guide for Identifying Contributors to Employee Errors*, LA-LP-02-199. Los Alamos, NM: Los Alamos National Laboratory, 2002.